A 'pearl' of Number Theory: the theorem of van der Waerden [1]

Sukumar Das Adhikari

Harish-Chandra Research Institute
Chhatnag Road, Jhusi, Allahabad 211 019, India
e-mail: adhikari@mri.ernet.in

1. Introduction. The theorem of van der Waerden, about which we are going to discuss here, is one among the 'pearls' that Khinchin presented [17] in his 'Three pearls of Number Theory'. As we shall see in this small expository article, this result has led to many interesting developments in Combinatorics and Number Theory.

Let $\mathbf{Z}^+$, be the set of positive integers.

If one considers the partition $\mathbf{Z}^+ = X \cup Y$, where

$$X = \left\{n \in \mathbf{Z}^+ : n \in [2^r, 2^{r+1}) \text{ for some even integer } r\right\}$$

and

$$Y = \left\{n \in \mathbf{Z}^+ : n \in [2^r, 2^{r+1}) \text{ for some odd integer } r\right\},$$

then it is clear that neither X nor Y will contain an infinite arithmetic progression.

However, we have the following [29]:

Theorem (van der Waerden). *Given positive integers k and r, there exists a positive integer $W(k,r)$ such that for any r-colouring of $\{1, 2, \ldots W(k,r)\}$, there is a monochromatic arithmetic progression (A.P.) of k terms.*

Here an *r-colouring* of a set S is a map $\chi : S \to \{c_1, \ldots, c_r\}$. Writing $S = \chi^{-1}(c_1) \cup \chi^{-1}(c_2) \cup \ldots \cup \chi^{-1}(c_r)$, an r-colouring of a set S is nothing but a partition of S into r parts where elements belonging to the same part receive the same colour. A subset A of S is called *monochromatic* if $A \subset \chi^{-1}(c_i)$ for some $i \in \{1, 2, \ldots, r\}$. Thus given an r-colouring $\chi : \mathbf{Z}^+ \to \{c_1, \ldots, c_r\}$, an A.P. $a, a+b, \ldots, a+kb$ will be monochromatic if $\chi(a) = \chi(a+b) = \cdots = \chi(a+kb)$.

The above theorem implies that for any finite partition $\mathbf{Z}^+ = X_1 \cup X_2 \cup \cdots \cup X_r$ of $\mathbf{Z}^+$, at least one X_i will contain arithmetic progression of any given length.

[1] Mathematics Newsletter, Vol. 18, No. 2, September 2008

We should remark that van der Waerden's Theorem is a Ramsey-type theorem. Ramsey Theory can be characterized as the subject dealing with results that talk about the phenomena of 'large' substructures of certain structures retaining certain regularities. Most often, we come across results saying that if a large structure is divided into finitely many parts, at least one of the parts will retain certain regularity properties of the original structure.

To our readers we recommend van der Waerden's personal account [30] of finding its proof. It contains the formulation of the problem with the valuable suggestions due to Emil Artin and Otto Schreier and depicts how the sequence of basic ideas occurred as an elaboration of the psychology of invention. It should also be mentioned that the result was originally (see [12] for instance) conjectured by Schur; since van der Waerden came to know it through Baudet, he calls it Baudet's conjecture.

At this point, it will be appropriate to mention one of the early Ramsey-type results due to Schur [24]:

Theorem (Schur). *For any r-colouring of $\mathbf{Z}^+$, $\exists$ a monochromatic subset $\{x, y, z\}$ of $\mathbf{Z}^+$ such that $x + y = z$. (The situation is described by saying that the equation $x + y = z$ has a monochromatic solution.)*

One observes that a three term arithmetic progression $x < y < z$ is a solution of the equation $x + z = 2y$ and by van der Waerden's theorem, for any finite colouring of $\mathbf{Z}^+$, this equation has a monochromatic solution. We remark that, in this direction, successful investigations of Rado ([20], [21], [22]) provided necessary and sufficient conditions for a system of homogeneous linear equations over $\mathbf{Z}$ to possess monochromatic solutions for finite colouring of $\mathbf{Z}^+$. One may look into [12] for Rado's theorem and some related results.

The following result [2] (see also [18], [1]) generalizes van der Waerden's Theorem to higher dimensions.

Theorem (Grünwald). *Let $d, r \in \mathbf{Z}^+$, the set of positive integers. Then given any finite set $S \subset (\mathbf{Z}^+)^d$, and an r-colouring of $(\mathbf{Z}^+)^d$, there exists a positive integer 'a' and a point 'v' in $(\mathbf{Z}^+)^d$ such that the set $aS + v$ is monochromatic.*

Remark. We note that when $d = 1$, one derives van der Waerden's Theorem by taking $S = \{1, \ldots, k\}$, in the above theorem.

In the next section we give an account of further developments along this theme. In the final section, we shall give a proof of Grünwald's Theorem.

2. Further developments. First, we discuss the theorem of Hales and Jewett [15] which reveals the combinatorial nature of van der Waerden's theorem. As has been said in [12]:

"the Hales-Jewett theorem strips van der Waerden's theorem of its unessential elements and reveals the heart of Ramsey theory".

So, this 'pearl of number theory' belongs to the ancient shore of Combinatorics! Indeed, van der Waerden's theorem was a prelude to a very important theme where interplay of several areas of Mathematics would be seen. Development of this theme, saw the results of Roth and Szemerédi and a number of different proofs of these results including the ergodic proof of Szemeredi's theorem due to Furstenberg. And, in the recent years, we have the results of Gowers and the Green-Tao Theorem.

We need some definitions before we can state Hales-Jewett Theorem.

Write

$$C_t^n = \{x_1x_2\dots x_n : x_i \in \{1, 2, \dots t\}\}.$$

In other words, C_t^n is the collection of words of length n over the alphabet of t- symbols $1, 2, \dots t$.

Then, by a *combinatorial line* in C_t^n we mean a set of t points in C_t^n ordered as $X_1, X_2, \dots, X_t$ where $X_i = x_{i1}x_{i2}\dots x_{in}$ such that for j belonging to a nonempty subset I of $\{1, \dots n\}$ we have $x_{sj} = s$ for $1 \leq s \leq t$ and $x_{1j} = \cdots = x_{tj} = c_j$ for some $c_j \in \{1, \dots t\}$ for j belonging to the complement (possibly empty) of I in $\{1, \dots n\}$.

For example, for $t = 3$ and $n = 5$, the following is a combinatorial line in C_3^5:

11122
21222
31322

Theorem (Hales-Jewett). *Given any two positive integers r and t, there exists a positive integer $n = HJ(r, t)$ such that if C_t^n is r-coloured then there exists a monochromatic combinatorial line.*

Observing the above example of the combinatorial line in C_3^5, and identifying the collection of words in C_3^5 with the set of integers in their usual expression in decimal system, it is easy to see that the above combinatorial line corresponds to a three term arithmetic progression with common difference 10100.

Thus, if we consider an r-colouring of C_t^n (with suitably large t), induced from a given r-colouring of the integers which have base d

representation with $d \geq t$, Hales-Jewett Theorem would imply the existence of a monochromatic arithmetic progression of t terms.

It was felt that, in the case of van der Waerden's theorem, while considering finite partition of $\mathbf{Z}^+$, only the 'size' of the part matters. Indeed, Erdős and Turan [6] conjectured that any subset of $\mathbf{Z}^+$ with positive upper natural density contains arithmetic progressions of arbitrary length, where, for $A \in \mathbf{Z}^+$, *the upper natural density* $\bar{d}(A)$ of A is defined by

$$\bar{d}(A) = \limsup_{N \to \infty} \frac{|A \cap [N]|}{N},$$

where $[N]$ denotes the set $\{1, 2, \ldots, N\}$.

We remark that in connection with Schur's theorem, the situation is quite different; though the set of even integers and the set of odd integers have the same upper natural density $1/2$ in $\mathbf{Z}^+$, there is no solution of $x + y = z$ in the subset of odd positive integers.

Towards the above mentioned conjecture of Erdős and Turan, in 1953 Roth [23] proved that any subset A of the set $\mathbf{Z}^+$ of positive integers with positive upper natural density will always contain a three-term arithmetic progression. Later, Szemerédi first improved [25] Roth's result to that of A possessing a four-term arithmetic progression and finally in 1974, in a famous paper [26] proved the general Erdös-Turan conjecture by a sophisticated combinatorial argument. Later, Furstenberg [7] gave an ergodic theoretic proof of Szemerédi's theorem which opened up the subject of Ergodic Ramsey Theory (see [8], [3] and [19]). There have been other important proofs of Szemerédi's theorem since then.

The area of Ergodic Ramsey Theory has many important developments which include the density version of the Hales-Jewett theorem by Furstenberg and Katznelson [9] and the polynomial extension of Hales-Jewett theorem by Bergelson and Leibman [4]. An expository account of the Bergelson-Leibman result is available in [3].

Defining $r_k(n)$ to be the smallest integer such that whenever $A \subset [n]$ satisfies $|A| > r_k(n)$, A contains an arithmetic progression of k terms, Szemerédi's result [26] implies that

$$r_k(n) = o(n).$$

For the case $k = 3$, Roth's proof [23] gave $r_3(n) = O\left(\frac{n}{\log \log n}\right)$; successive improvements in this direction were obtained by Heath-Brown

[16], Szemerédi [27] and Bourgain [5], the result of Bourgain being

$$r_3(n) = O\left(n \cdot \sqrt{\frac{\log\log n}{\log n}}\right).$$

Regarding estimates of $r_k(n)$ for $k > 3$, Gowers [10] has made a remarkable breakthrough while establishing

$$r_4(n) < \frac{n}{(\log\log n)^d} \text{ for some absolute constant } \ d > 0,$$

where the method seems to go through for $r_k(n)$ for $k \geq 4$.

Apart from the original paper [10], we recommend the two beautiful articles [11] and [5] for getting an idea as well as the background of the proof.

The following conjecture of Erdős is still open.

Conjecture (Erdős). If $A \subset \mathbf{Z}^+$ satisfies

$$\sum_{a \in A} \frac{1}{a} = \infty,$$

then A contains arithmetic progressions of arbitrary length.

Recently, in the Green-Tao Theorem [14] we have seen a major breakthrough. Green and Tao showed that the set of primes contains arithmetic progressions of arbitrary length.

We refer to [28] and [13] for an accessible account of the recent developments in the area of Additive Combinatorics; the reader will find the extensive bibliography provided in those volumes very helpful.

3. Proof of Grünwald's Theorem.

We work with fixed d. Now, the theorem will be proved if we prove the following statement for all finite sets $S \subset (\mathbf{Z}^+)^d$.

$A(S)$: For each $k \in \mathbf{Z}^+$, $\exists\ n = n(k)$ such that for every k-colouring of $B_n \stackrel{def}{=} \{(a_1, \ldots, a_d) : a_i \in \mathbf{Z}^+, 1 \leq a_i \leq n\}$, B_n contains a monochromatic subset of the form $aS + v$ for some $a \in \mathbf{Z}^+$ and $v \in B_n$.

We remark that the above statement not only proves the theorem, given the number of colours used and the given set S, it tells us (as in our statement of van der Waerden's theorem) about the size of the finite cube where the monochromatic subset of the form $aS + v$ can be found. In fact, by the 'Compactness Principle' (see [12], for instance), the above statement is equivalent to the statement in the theorem; we shall not go into this.

Since $A(S)$ is obviously true if $|S| = 1$, it is enough to show that $A(S) \Rightarrow A(S \cup \{s\})$ for any $s \in (\mathbf{Z}^+)^d$.

For the induction procedure, once $A(S)$ is established for a given S, we prove the the following intermediate statement $C(p)$ corresponding to a positive integer p. Once $C(p)$ is established for any positive integer p, it will lead to the statement $A(S \cup \{s\})$ and we shall be through.

$C(p)$: Let $S \subset (\mathbf{Z}^+)^d$ be fixed for which $A(S)$ is true. Then for given $k \in \mathbf{Z}^+$ and $s \in (\mathbf{Z}^+)^d$, $\exists n = n(p,k,s) \in \mathbf{Z}^+$ such that for each k-colouring of B_n, there are positive integers $a_0, a_1, \ldots, a_p$ and a point $u \in (\mathbf{Z}^+)^d$ such that the each of the $(p+1)$ sets

$$T_q \stackrel{\text{def}}{=} u + \sum_{0 \le i < q} a_i S + \left(\sum_{q \le i \le p} a_i \right) s, \ 0 \le q \le p,$$

are monochromatic subsets of B_n.

$C(0)$ holds trivially and we have to show that $C(p) \Rightarrow C(p+1)$.

Let $n = n(p,k,s)$ be the integer specified for $C(p)$. Now, given a k-colouring of $(\mathbf{Z}^+)^d$, we define the *associated colouring* of $(\mathbf{Z}^+)^d$ such that two points u and v will have the same colour in this new colouring iff the lattice points in the cubes $u + B_n$ and $v + B_n$ are identically coloured in the original k- colouring of $(\mathbf{Z}^+)^d$.

Clearly, this associated colouring of $(\mathbf{Z}^+)^d$ is a k'- colouring where $k' \stackrel{\text{def}}{=} k^{n^d}$.

Now, from $A(S)$, it follows that $\exists$ an integer $n' = n'(k')$ such that for every k'-colouring of $B_{n'}$, $B_{n'}$ contains a monochromatic subset of the form $a'S + v'$ for some $a'(\neq 0) \in \mathbf{Z}^+$ and $v' \in B_{n'}$.

Let $N = n + n' + 1$. Let a k-colouring of B_N be given. In an arbitrary way we extend this to a k-colouring of $(\mathbf{Z}^+)^d$. Now, corresponding to the associated k'- colouring of $(\mathbf{Z}^+)^d$, $B_{n'}$ contains a monochromatic subset of the form $a'S + v'$. This means that the $|S|$-cubes $B_n + a't + v', t \in S$ are coloured identically in the original k-colouring. We observe that all these cubes lie in B_N. By $C(p)$, for any $t \in S$, the cube $B_n + a't + v'$ contains monochromatic sets

$$T_q(t) = a't + v' + u + \sum_{0 \le i < q} a_i S + \left(\sum_{q \le i \le p} a_i \right) s, \ 0 \le q \le p.$$

Setting $b_0 = a'$ and $b_i = a_{i-1}$, $1 \le i \le p+1$, we claim that the sets

$$T'_q = (v' + u) + \sum_{0 \le i < q} b_i S + \left(\sum_{q \le i \le p+1} b_i \right) s, \ 0 \le q \le p+1$$

are monochromatic.

For $q = 0$,

$$T_0' = (v' + u) + \left(\sum_{0 \le i \le p+1} b_i \right) s$$

is a singleton and the claim is established.

For $q \ge 1$, $T_q' = \cup_{t \in S} T_{q-1}(t)$. Since $B_n + a't + v'$ are identically coloured for different t's belonging to S, it follows that the monochromatic sets $T_{q-1}(t)$ are of the same colour and hence $T_q' = \cup_{t \in S} T_{q-1}(t)$ is a monochromatic subset of B_N.

Thus $C(p+1)$ holds with $n(p+1, k, s) = N$.

Now that $C(p)$ is established for all integers $p \ge 0$, the particular case $p = k$ gives us an integer $n = n(k, k, s)$ such that given any k-colouring of B_n, $\exists (k+1)$ monochromatic sets $T_0, \ldots, T_k$ in B_n. By pigeonhole principal, two of these sets, say T_r, T_q with $r < q$ are of the same colour.

Writing

$$T_r = u + \sum_{0 \le i < r} a_i S + \left(\sum_{r \le i < q} a_i \right) s + \left(\sum_{q \le i < k+1} a_i \right) s$$

and

$$T_q = u + \sum_{0 \le i < r} a_i S + \sum_{r \le i < q} a_i S + \left(\sum_{q \le i < k+1} a_i \right) s,$$

and choosing $s_0 \in S$ (S being nonempty), it follows that the set

$$T = u + \left(\sum_{0 \le i < r} a_i \right) s_0 + \left(\sum_{r \le i < q} a_i \right) (S \cup \{s\}) + \left(\sum_{q \le i < k+1} a_i \right) s$$

is contained in B_N and is monochromatic.

Setting $a = \sum_{r \le i < q} a_i$ and $v = u + \left(\sum_{0 \le i < r} a_i \right) s_0 + \left(\sum_{q \le i < k+1} a_i \right) s$, $T = a(S \cup \{s\}) + v$ and this establishes $A(S \cup \{s\})$.

References

[1] S. D. Adhikari, *Aspects of combinatorics and combinatorial number theory*, Narosa, New Delhi, 2002.

[2] P. G. Anderson, *A generalization of Baudet's conjecture (van der Waerden's Theorem)*, Amer. Math. Monthly, **83**, 359–361, (1976).

[3] V. Bergelson, *Ergodic Ramsey Theory - an Update*, London Mathematical Society Lecture Note Series 228, Cambridge University Press, 1996.

[4] V. Bergelson and A. Leibman, *Set-polynomials and polynomial extension of the Hales-Jewett theorem*, Ann. of Math. (2) **150**, no. 1, 33–75 (1999).

[5] J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal., **9**, no. 5, 968–984 (1999).

[6] P. Erdős and P. Turan, *On some sequences of integers*, J. London Math. Soc. **11**, 261–264 (1936).

[7] H. Furstenberg, *Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. d'Analyse Math. **31**, 204–256 (1977).

[8] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton University Press, 1983.

[9] H. Furstenberg and Y. Katznelson, *A density version of the Hales-Jewett theorem*, J. Analyse Math., **57**, 64–119 (1991).

[10] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, GAFA, **8**, 529–551 (1998).

[11] W. T. Gowers, *Fourier analysis and Szemerédi's theorem*, Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998). Doc. Math., Extra Vol. I, 617–629 (1998).

[12] R. L. Graham, B. L. Rothschild and J. H. Spencer, *Ramsey Theory*, John Wiley & Sons, 1980.

[13] A. Granville, M. B. Nathanson and J. Solymosi (Eds.), *Additive Combinatorics*, CRM Proceedings and Lecture Notes, Volume 43, American Mathematical Society, 2007.

[14] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math., to appear.

[15] A. W. Hales and R. I. Jewett, *Regularity and positional games*, Trans. Amer. Math. Soc. **106**, 222–229 (1963).

[16] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. (2) **35**, 385–394 (1987).

[17] A. Y. Khinchin, *Three Pearls of Number Theory*, Graylock Press, 1952.

[18] M. Lothaire, *Combinatorics on Wards*, Addison - Wesley, 1983.

[19] R. McCutcheon, *Elemental methods in ergodic Ramsey theory*, Springer, Lect. Notes Math., **Vol. 1722**, 1999.

[20] R. Rado, *Verallgemeinerung eines Satzes von van der Waerden mit Anwendungen auf ein problem der Zalentheorie, Sonderausgabe aus den Sitzungsbericten der Preuss*, Akad. der Wiss. Phys. -Math. klasse **17**, 1–10 (1933).

[21] R. Rado, *Studien zur Kombinatorik*, Math. Z. **36**, 424 –480 (1933).

[22] R. Rado, *Some recent results in combinatorial analysis*, Congrès International des Mathematiciens, Oslo, 1936.

[23] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28**, 104–109 (1953).

[24] I. Schur, *Über die Kongruenz* $x^m + y^m \equiv z^m \pmod{p}$, Jber. Deutsch. Math. Verein. **25**, 114–117 (1916).

[25] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression*, Acta. Math. Acad. Sci. Hungar. bf 20, 89–104 (1969).

[26] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta. Arith. bf 27, 199–245 (1975).

[27] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta. Math. Hungar.,**56**, 155–158 (1990).

[28] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.

[29] B. L. van der Waerden, *Beweis einer Baudetschen Vermutang*, Nieuw Arch. Wisk. **15**, 212–216 (1927).

[30] B. L. van der Waerden, *How the proof of Baudet's conjecture was found*, Studies in Pure Mathematics (Edited by L. Mirsky), Academic Press, 251–260 (1971).